

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v.

Case No.: _____

SKYRYSE, INC., ROBERT ALIN
PILKINGTON, MISOOK KIM, and DOES NOS.
1-50,

Defendants.

DECLARATION OF BRUCE W. PIXLEY

BRUCE W. PIXLEY, under penalty of perjury and pursuant to 28 U.S.C. § 1746,
declares the following to be true and correct:

I. Background

1. My name is Bruce W. Pixley. I provide this declaration in support of Moog Inc.'s Motion for a Temporary Restraining Order/Preliminary Injunction. I am over the age of 18 years. I have personal knowledge of the matters set forth herein and if called as a witness, I could and would competently testify as to all facts set forth herein.

2. I am the Managing Member of Pixley Forensics Group LLC. My responsibilities include assisting corporate clients and law firms in investigations and disputes involving forensic accounting issues, electronic discovery, theft of intellectual property, and computer forensic investigations. In this capacity, I manage teams of forensic examiners and use a variety of technologies to perform data acquisition and analysis of this information.

3. Since 2001, I have served as a lead instructor of computer forensics, Internet investigations, and network intrusion courses for the California Department of Justice's Advanced Training Center. Additionally, I have been employed as a Master Instructor at Guidance Software, which developed the EnCase computer forensic software. As an instructor, I have taught for over 2,000 hours on the subjects of computer forensics and high-tech investigations. I have developed course training materials and wrote manuals for computer forensic courses such as Advanced Internet Examinations and Network Intrusion Investigations.

4. I possess three professional certifications for my fields of work. I possess the Certified Information Systems Security Professional (CISSP) certification and the GIAC Certified Forensic Analyst (GCFA) certification, which are both ANSI ISO accredited credentials, and the EnCase Certified Examiner certification.

5. Since 2003, I have been retained as a computer forensic examiner and subject matter expert in both criminal and civil matters. I have been qualified as an expert witness in both state and federal courts and testified about the foundation of computer forensics, Windows and Mac operating systems, chat software, Internet and network operations, e-mail, peer-to-peer file sharing, digital photography, recovery of deleted data, and Trojan viruses.

6. Attached as **Exhibit A** to this declaration is a copy of my current Curriculum Vitae, which sets forth in detail additional aspects of my qualifications and background.

7. I have been retained by Sheppard, Mullin, Richter & Hampton LLP, counsel for Moog Inc. ("Moog" or "Company") to conduct a forensic analysis of certain company-issued laptop computers and external storage drives for any evidence of the exfiltration of Company data.

II. Summary of Opinions and Findings

8. As set forth in Sections D below, I have come to the following opinions regarding my analysis of the laptop hard drive:

a. Company data belonging to Moog was intentionally copied from company-issued laptop computers by a user account assigned to Misook Kim to an external USB storage device on at least two separate occasions in November and December 2021.

b. The use of external USB storage devices allows a former employee to access the company's data from any computer in the world. Once accessed, the data can be viewed, printed, manipulated, imported into other files, transferred to other people, and backed up to another computer or storage device.

c. The Samsung USB storage device returned by Misook Kim on February 21, 2022 had been intentionally formatted, which wiped all previously used sectors of data, making the data unrecoverable, and replaced those sectors with zeroes. This formatting also prevents Moog from determining whether the underlying data was copied or transferred to another location or device. This destructive act occurred sometime after December 17, 2021 and before February 21, 2022.

III. Employee Pattern of Conduct

9. In my years of experience conducting computer forensic examinations, specifically theft of company data and trade secrets, I have found that employees who were in the process of leaving their employment would intentionally take the company's electronic data with them so that they could continue to use that data to their benefit, and to the detriment of the former employer. These investigations often involved the use of external USB storage devices.

The use of USB storage devices is simple and an inexpensive means to exfiltrate company data and the employees would retain the data after they departed their employment.

10. A USB storage device allows the employee to access this data from any computer in the world. Once accessed, the data can be viewed, printed, manipulated, imported into other files, transferred to other people, and backed up to another computer or storage device. Since these methods offer the employee multiple options, it is difficult to track and quarantine the company data.

IV. Evidence Reviewed and Methodology

11. On March 1, 2022, I received a comma-delimited log (“Ivanti Log”) from Moog.

12. On March 1, 2022, I received a FedEx package, tracking number 776160614737, from Setec Investigations. The package contained an encrypted hard drive that stored forensic images of the following devices:

a. Dell Latitude 7480 laptop computer (Service Tag FGPYGH2), hereafter referred to as “Dell Laptop 1”;

b. Dell Precision 7540 laptop computer (Service Tag 9S4Z433), hereafter referred to as “Dell Laptop 2”;

c. Samsung USB solid state storage drive (T7 series, model MU-PC1T0H, serial number S5SXNS0R702326Z), hereafter referred to as “Samsung USB Storage 1”;
and

d. Western Digital USB external drive (model: MyPassport, 3TB, serial number WX31DB63EDS5), hereafter referred to as “Western Digital Drive.”

13. I understand that Dell Laptop 1 and Dell Laptop 2 were company-issued computers that were assigned to Misook Kim, who is a former employee whose last day of employment was December 17, 2022.

14. Prior to my analysis, I verified the integrity of the forensic images listed above. Each image verified successfully with zero errors reported.

15. I conducted an analysis of the forensic images using the following computer forensic software:

- a. X-Ways version 20.4;
- b. Forensic Explorer version 5.4.8;
- c. Axiom version 5.8; and
- d. Tzworks version 2021.12.10.

V. Details of Analysis and Findings

16. My analysis of the Dell Laptop 1 and Dell Laptop 2 consisted of reviewing file and drive activity and files maintained by the operating system. The operating system files included, but were not limited to, the registry, shortcuts (.lnk files), jumplists, and log files.

Operating System Information

17. I reviewed the forensic image of Dell Laptop 1 for basic operating system information and found the following:

- a. The installed operating system was running Windows 10 Enterprise and had been assigned the computer name of “USTO1LPFGPYGH2”; and,
- b. The Windows 10 operating system included a user folder for a Windows domain user account called “mkim3,” which was assigned to Misook Kim.

18. I reviewed the forensic image of Dell Laptop 2 for basic operating system information and found the following:

a. The installed operating system was running Windows 10 Enterprise and had been assigned the computer name of “USTO1LP9S4Z433”; and,

b. The Windows 10 operating system included a user folder for a Windows domain user account called “mkim3,” which was assigned to Misook Kim.

Connection of Samsung USB Storage Devices

19. Based on my analysis of Dell Laptop 1 and Dell Laptop 2, I discovered that Samsung USB Storage 1 had been connected on the following dates:

a. Dell Laptop 1: September 13, 2021 and November 19, 2021;

b. Dell Laptop 2: September 25, 2021 and December 15, 2021.

20. During my analysis of Dell Laptop 2, I discovered that a second Samsung USB solid state storage device (Series T7, serial number S5SXNS0R700159M) had been connected on the following dates: September 27, 2021; September 28, 2021; November 22, 2021; November 28, 2021; and November 29, 2021. I understand that this device has not been located or returned to Moog.

Evidence of Copying Data to Samsung USB Storage Drive

21. I understand that Moog had installed third-party endpoint software (“Ivanti Software”) on each computer that is specifically designed to capture user-related file transfer (copying) activity from the computer to an external USB storage device, such as the Samsung USB Storage 1. The Ivanti Software captures information such as the user name, the computer name, the USB storage device information, the file name, the destination folder, and the transfer

date and time. This captured information is sent to a database server maintained by Moog. Once the information is stored in the database, it can be exported as a log and analyzed.

22. I received the Ivanti Log that listed file copying activity associated with Misook Kim's user account on Dell Laptop 1 on November 19, 2021, a true and correct copy of which is attached as Exhibit A to the concurrently filed Declaration of Ian Bagnald. The file copying began at 3:34 a.m. PST, which was 18 minutes after Samsung USB Storage 1 was connected at 3:16 a.m. PST.

23. The Ivanti Log showed that a total of 136,994 files were copied to a primary subfolder on Samsung USB Storage 1 called "Misook" during a 4 hour time frame (3:34 a.m. to 7:33 a.m. PST). The total volume of data that was copied was approximately 139 gigabytes.

Microsoft OneNote Notebook Data

24. During my analysis of Dell Laptop 2, I found evidence that the "Misook" folder still existed on the Samsung USB Storage 1 device when it was connected on December 15, 2021.

25. Additionally, a new folder and data was added to the "Misook" folder on the Samsung USB Storage 1 on December 15, 2021 called "OneNote Notebooks." Microsoft OneNote is a program that is used to store user's notes, drawings, and screen shots. A user can organize and store this information in multiple digital notebook files.

26. I searched Dell Laptop 2 for any OneNote data and found that a folder called "OneNote Notebooks" had been stored in Misook Kim's Documents folder (Users\mkim3\Documents\Misook\OneNote Notebooks). This folder contained over 200 digital notebook files.

27. Two days later on December 17, 2021, at 11:39 a.m. PST, the entire “Misook” folder (Users\mkim3\Documents\Misook) on Dell Laptop 2 that included the OneNote Notebook data was deleted. The deleted “Misook” folder contained approximately 54 GB of data. It should be noted that this folder deletion was an intentional user deletion of data and the data was not transferred to the user’s Recycle Bin folder where it could be easily recovered.

Destruction of Data on Samsung USB Storage Device

28. I analyzed the forensic image of Samsung USB Storage 1. I confirmed that the serial matched on the device matched the same Samsung USB storage device connected to Dell Laptop 2 on December 15, 2021.

29. At an unknown time after Misook Kim departed Moog on December 17, 2021, someone intentionally formatted Samsung USB Storage 1 with the exFAT file system. This process was intentional, destructive, and obscured my ability to recover any data on the drive. When a hard drive is formatted, it needs to be connected to a computer to start and complete the process. At the start of the formatting process, a user has choices to set options on how the drive will be formatted. In this case, the user selected the option to force the formatting process to overwrite and wipe all sectors on the drive with zeroes. Not only is formatting a drive an intentional act, but this specific formatting process effectively wiped all previous data on the drive so all previous data would be unrecoverable.

30. Since the Samsung USB Storage 1 device was formatted and wiped, I am unable to determine:

- a. What computers the device may have been connected to after December 17, 2021; and

b. When or how anyone may have accessed, copied, transferred, modified, or otherwise exported the data on the drive after it was removed from Moog on December 17, 2021.

False Impression of the Western Digital Drive

31. Samsung USB Storage 1 had a volume name of “Misook-T7” prior to the drive being reformatted. A volume name is an arbitrary name that can be set by the user. This volume name was captured by both Dell Laptop 1 and Dell Laptop 2. When a drive is reformatted, the user has the option to keep the volume name intact. In this case, the volume name was still set to “Misook-T7.”

32. When I analyzed the forensic image of the Western Digital Drive returned to Moog on January 31, 2022, I discovered that the volume name had been set to “Misook T7,” which is very similar (sans the hyphen) to the volume name set on Samsung USB Storage 1. During my analysis of Dell Laptop 1 and Dell Laptop 2, I did not locate any evidence of the Western Digital Drive being connected to either computer. Based on the similar volume names, the volume name of the Western Digital Drive (“Misook T7”) would create the false impression that it was the original drive connected to both Dell Laptop 1 and Dell Laptop 2. However, the Windows operating system tracks additional information about external USB drives, such as make, model, and serial number. This additional information captured by the operating system provided the foundation that the Western Digital Drive was not the drive used to copy data from Dell Laptop 1 and Dell Laptop 2.

VI. Conclusions

33. Company data belonging to Moog was intentionally copied from a company-issued laptop computer by a user account assigned to Misook Kim to Samsung USB Storage 1 on November 19, 2021 and December 15, 2021.

34. The use of external USB storage devices allows a former employee to access the company's data from any computer in the world. Once accessed, the data can be viewed, printed, manipulated, imported into other files, transferred to other people, and backed up to another computer or storage device.

35. All data on Samsung USB Storage 1 was intentionally wiped during a reformatting process by an unknown person after Misook Kim departed Moog on December 17, 2021 and the time the drive was returned to Moog on February 21, 2022. This prevented any analysis on the device in an effort to determine what files were copied, accessed, transferred or modified after December 17, 2021 and what computers the device may have been connected to.

I declare that the foregoing is true and correct under penalty of perjury under the laws of the United States of America.

Dated: March 5, 2022

A handwritten signature in black ink, appearing to read 'B. Pixley', is written over a horizontal line.

Bruce W. Pixley